IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ADDRESSES THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE, YAHOO, AMAZON, AND NAMECHEAP	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kathryn Thibault, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for four search warrants for information associated with certain accounts that are stored at premises controlled by (i) Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California; (ii) Yahoo!, Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California; (iii) Amazon, an email provider headquartered at 300 Deschutes Way SW, Ste. 304, Tumwater WA 98501, and (iv) NameCheap, an email provider headquartered at 11400 W. Olympic Boulevard, Suite 200, Los Angeles, CA 90064. The information to be searched is described in the following paragraphs and in Attachments A. This affidavit is made in support of an application for four search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Yahoo, Amazon, and NameCheap to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), reporting to the Boston, Massachusetts Division, and have been employed by the FBI since October 1998. I

am currently assigned to the Bedford Resident Agency of the FBI and am assigned to work a myriad of white collar crime cases. I am familiar with the tactics, methods and techniques of people who commit bank fraud, money laundering and illegally act as unlicensed money transmitting businesses. I have attended numerous federal agency and private sponsored training courses all over the United States. In June 2017, I attended an on-line networking and enterprise training conference in Atlanta, Georgia where topics such as crypto currency, use of e-mail in money laundering cases and the "dark" web were topics of instruction.

3. As a Special Agent with the FBI, I am responsible for conducting criminal investigations involving violations of Title 18 of the United States Code and other federal statutes enforced by the FBI. Based upon my experience participating in cases involving bank fraud, money laundering and unlicensed money transmitting businesses, I know that businesses which transmit money affecting interstate commerce and operate without an appropriate money transmitting license, fail to comply with the business registration requirements under 31 U.S.C. § 5330 and are therefore unlicensed money transmitting businesses.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money transmitting business, and of 18 U.S.C. §§1956 and 1957, which prohibit money laundering (together, "the Target Offenses"), have been committed by Ian Freeman ("Freeman") and other unknown persons. There is also probable cause to search the

information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATUTES

7. Title 18, United States Code, Section 1960 provides, in relevant part, that

> Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

18 U.S.C. § 1960(a). The term "unlicensed money transmitting business" means "a money transmitting business which affects interstate or foreign commerce in any manner or degree" and

> (A) "is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable";
>
> (B) "fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section"; or
>
> (C) "otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."

18 U.S.C. § 1960(b)(1).

8. Title 18, United States Code, Section 1956 provides, in relevant part, that

> Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified

> unlawful activity . . . with the intent to promote the carrying on of specified unlawful activity; or . . . knowing that the transaction is designed in whole or in part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or . . . to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine . . . or imprisonment for not more than twenty years, or both.

18 U.S.C. § 1956(a)(1).

9. Title 18 United States Code, Section 1956(a)(2) provides, in relevant part, that

> Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States . . . with the intent to promote the carrying on of specified unlawful activity; or . . . knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or (ii) to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine . . . or imprisonment for not more than twenty years, or both.

18 U.S.C. § 1956(a)(2).

PROBABLE CAUSE

10. I am investigating a group, led by Ian Freeman, that operates unlicensed Bitcoin ATMs and uses other means to exchange cash for Bitcoin throughout New Hampshire. There is probable cause to believe that in doing so, Freeman and his associates are operating an unlicensed money transmitting business. In addition, I have determined that substantial amounts of the cash that Freeman and his group convert to Bitcoin represent the proceeds of fraudulent schemes like romance scams. I believe that scammers may use Freeman's unlicensed ATMs, or take advantage of other services he offers, to convert the proceeds of their scams to Bitcoin. As described below, there is probable cause to believe that Ian Freeman is committing the Target Offenses by running an unlicensed business in which customers and fraud victims exchange cash for digital currency

(including Bitcoin) for a fee, and that he knowingly engages in financial transactions involving the proceeds of his unlicensed business.

11. As described further below, our investigation has revealed that in committing the Target Offenses, Freeman or his associates use the following email accounts:

- Keenecrypto@gmail.com
- Bitcoinbombshell727@gmail.com
- Shirebtc+lbc@gmail.com
- Shirecryptocoin@gmail.com
- Shirebtc@gmail.com
- Shirebtc-itbit@gmail.com
- Ian+gemini@freetalklive.com
- Ian@freetalklive.com
- Chaosdragoon77@yahoo.com
- Steven@anypayinc.com

The application accompanying this affidavit requests warrants to search these accounts. I have been assisted in this investigation by agents of the Internal Revenue Service ("IRS") and the United States Postal Inspection Service ("USPIS").

Background About Bitcoin

12. Based on my training and experience as a financial investigator and the investigation to date, I know that Bitcoin (BTC)[1] is a type of virtual currency, circulated over the internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency. Other virtual currency includes Bitcoin Cash ("BCH"), Litecoins ("LTC"), Ethereum ("ETH" or "ether"), and Ripple (XRP). For ease of reference, the

[1] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

analysis below relating to Bitcoin generally applies to other types of cryptocurrencies (often collectively referred to as "Altcoins").

13. According to Section 1.3 of FinCEN Guidance, FIN-2019-G001, dated May 9, 2019, and available at https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (the "2019 FinCEN Guidance"[2]), the term "virtual currency" refers to a medium of exchange that can operate like currency but does not have all the attributes of "real" currency, as defined in 31 CFR § 1010.100(m), such as legal tender status.

14. A convertible virtual currency or "CVC" is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency." 2019 FinCEN Guidance § 1.3.[3] CVCs include "digital currency" or "cryptocurrency" such as bitcoin.

15. Bitcoin are sent to and received from BTC "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the Bitcoin address. Only the holder of an address' private key can authorize any transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple

[2] FinCEN, the Financial Crimes Enforcement Network, is the regulatory authority and law enforcement agency of the US Treasury Department responsible for establishing and implementing polices to detect money laundering.

[3] FinCEN regulations define the term "money transmission services" to mean the "acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." 31 CFR § 1010.100(ff)(5)(i)(A). The term "other value that substitutes for currency" encompasses situations in which the transmission does not involve currency, 31 CFR § 1010.100(m), or funds, but instead involves something that the parties to a transaction recognize has value that is equivalent to or can substitute for currency.

BTC addresses at any given time and may use a unique Bitcoin address for each and every transaction.

16. To acquire bitcoin, a typical user purchases them from a virtual[4] currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities and must maintain a record of the identity of any customer involved in a transmission of funds of $3,000 or more.[5] Such businesses must also file Suspicious Activity Reports with FinCEN when appropriate, including reporting substantial transactions or patterns of transactions involving the use of the money service business to facilitate criminal activity.[6]

17. One type of virtual currency exchange is a "CVC kiosk." CVC kiosks—which are also referred to as "CVC automated teller machines (ATMs)" or "CVC vending machines"—are "electronic terminals that act as mechanical agencies of the owner-operator, to enable the owner-operator to facilitate the exchange of CVC for currency or other CVC." 2019 FinCEN Guidance § 4.3. According to FinCEN, "[a]n owner-operator of a CVC kiosk who uses an electronic

[4] Bitcoins can accurately be referred to as a virtual, digital, and/or cryptographic currency.

[5] See 31 C.F.R. §§ 1010.410, 1022.400, 1022.210(d)(i)(A).

[6] See 31 C.F.R. § 1022.320.

terminal to accept currency from a customer and transmit the equivalent value in CVC (or vice versa) qualifies as a money transmitter both for transactions receiving and dispensing real currency or CVC." Id. [7] Thus, "owners-operators of CVC kiosks that accept and transmit value must comply with FinCEN regulations governing money transmitters." Id.

18. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to-peer BTC network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflects any identifying information about either sender or recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

19. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can sometimes trace transactions to third party companies that collect identifying information about their customers and are responsive to legal process.

---

[7] See also 31 C.F.R. §1010.100(ff)(5); Department of the Treasury Financial Crimes Enforcement Network Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013, FIN-2013-G001, available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

20. Software called "blockchain explorers" can be used to view and analyze the blockchain. Blockchain analysis using a blockchain explorer can help link Bitcoin transactions to an exchange service and is a key way of associating an unknown or anonymous Bitcoin user with a real world identity.

21. While virtual currency is not, in itself, illegal and is known to have legitimate uses, I also know, in my training and experience, that virtual currency like bitcoin is used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move money anonymously.

22. I am aware that individuals conducting business with virtual currencies must use a computer or other electronic device, such as a smartphone, tablet, or computer to conduct transactions involving bitcoin. Users of bitcoin must establish electronic wallets to receive and send the bitcoin during these transactions. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, or computers. They may also be stored on third party wallet providers (such as Armory). Individuals often associate email accounts with these wallet providers and store information relating to that wallet on their email account. I am also aware that individuals conducting business by bitcoin can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. They are also often stored on email accounts, cloud or shared drives stored online (such as Google Drive), and other online storage mediums.

The Investigation

23. According to public records, Ian B. Freeman was born "Ian Bernard." Around November 7, 2013, he changed his last name to Freeman. Subpoenaed records from some of Freeman's bank accounts contain applications in which Freeman describes himself as a "Cyrptocurrency Minister," and as a member of the Shire Free Church. Various online postings and public records also link Freeman to the Shire Free Church.[8] According to Freeman's Twitter account, @FTL_Ian, Freeman is a "Peace Minister of the Shire Free Church" and the host of Free Talk Live. Freeman identifies himself through postings as the user of this Twitter account. Numerous bank records associated with Freeman's accounts list him as a minister or a cryptocurrency minister. Freeman is also a blogger on the FreeKeene.com website.

24. According to corporate record searches with the Secretary of State Offices, the Shire Free Church Holdings, LLC has an address of 63 Emerald Street, Suite 610 in Keene, NH. I have confirmed that 63 Emerald Street is the address of "The Shipping Shack," which according to the website, https://shippingshack.com/, is an authorized packing and shipping center for DHL, UPS, USPS and FEDEX with 24-hour mailbox access.

25. According to his New Hampshire Driver's license, IAN Freeman resides at 73 Leverett Street in Keene, New Hampshire. According to the City of Keene, New Hampshire Property and Tax Assessment Department this address, 73-75 Leverett Street in Keene appears to be a duplex or two units. This property was originally purchased by Ian Bernard aka Ian Freeman on May 19, 2006.

[8] The Shire Free Church is not, to my knowledge, a recognized religious entity for tax purposes. In 2014, Keene voted to deny the group's application for tax exempt status. It is not recognized as tax exempt with the IRS either.

Freeman's Importation of CVC Kiosks

26. According to records from U.S. Customs and Border Protection, a CVC kiosk was delivered to the Bitcoin Embassy NH, also known as Route 101 Goods, which is located at 661 Marlboro Road, Keene, New Hampshire. According to the Bitcoin Embassy NH website, https://bitcoinembassynh.org/index.php/about-the-embassy and the Bitcoin Embassy NH Facebook Page, this embassy is located at 661 Marlboro Road, Keene, New Hampshire. According to www.freekeene.com, "Keene's first Bitcoin Vending Machine launched at what was then a thrift store at 661 Marlboro Rd (Rt. 101 across from Cheshire Oil). The machine is part of the Shire Free Church's project to spread cryptocurrency in the region." Route 101 Goods, The Bitcoin Embassy, and the Shire Free Church are all associated with each other through this CVC kiosk located at 661 Marlboro Road, Keene, New Hampshire.

27. In fact, according to records from U.S. Customs and Border Protection ("CBP") reviewed by FBI analysts in Washington, D.C., at least eight CVC kiosks have been imported to New Hampshire and received by entities or individuals associated with Freeman. A public source website lists the contact information associated with each of the CVC kiosks, displayed in the below chart.

Kiosk Location Name	**Kiosk Operator's Name**	**Address**	**Support E-mail**
Thirsty Owl	Shire Free Church	141 Winchester Street, Keene, NH 03431	**keenecrypto@gmail.com**[9]
Seacoast Rep Theater	Shire Bitcoin	125 Bow Street, Portsmouth, NH 03801	**steven@anypayinc.com**
Murphy's Taproom	Shire Free Church	494 Elm Street, Manchester, NH 03101	**keenecrypto@gmail.com**

[9] I have highlighted email addresses that are the subject of this search warrant affidavit in bold type.

Port City Coin & Jewelry	Shire Bitcoin	599-US1, Portsmouth, NH 03801	**steven@anypayinc.com**[10]
Area 23	Shire Cryptocoin	254 N State Street, Concord, NH 03301	**shirecryptocoin@gmail.com**
Bitcoin Embassy NH	Shire Free Church	661 Marlboro Road, Keene, NH 03431	**keenecrypto@gmail.com**

28. A prior search on the public source website listed a seventh CVC kiosk at the Free State Bitcoin Shoppe, 56 State Street, Portsmouth, NH 03801, operated by "Shire Bitcoin." On November 22, 2019, investigators searched for this kiosk on the public source website and it is no longer registered. Investigators have not identified the location of the eighth CVC kiosk.

29. Investigators identified several of these CVC kiosks as being purchased from GeneralBytes by Ian Freeman or his associates. GeneralBytes is a company which, according to its website, https://www.generalbytes.com/aboutus/, is the "world's largest Bitcoin, Blockchain and Cryptocurrency ATM manufacturer." According to the website, GeneralBytes' main offices are located in the Czech Republic and it has satellite offices in Florida.

30. Records from GeneralBytes include sales agreements with the Shire Free Church in Manchester, New Hampshire, represented by Ian Freeman. The records include invoices for the devices purchased (including various of the CVC kiosks described above) and indicate that the devices were sent to various addresses in New Hampshire at Freeman's instruction.

[10] According to open source web based domain search sites, the email account ending in the "anypayinc.com" registered domain is hosted by NameCheap. A domain name is a set of characters that identifies a website. When the domain name is entered into a web browser, the domain name server (DNS) will provide the location of the affiliated website and display it. When the website is accessed on the internet it has an Internet Protocol (IP) address associated with it. Further review shows that the IP associated with the "anypayinc.com" domain appears to be hosted through Amazon Web Services, Inc. Therefore, I believe that records associated with this email address will be retained by both NameCheap and Amazon.

31. GeneralBytes also provided the e-mail addresses used to communicate with Freeman and provided by Freeman throughout the transaction agreements. The e-mail addresses used for the primary communications between Freeman and GeneralBytes were **ian@freetalklive.com**, bvm5ne@gmail.com, and shirebtcmanch@googlegroups.com. For example, GeneralBytes produced a sales agreement, dated July 5, 2016, to purchase CVC kiosks. The contract was initialed by IF (Ian Freeman) on December 23, 2015. Freeman initialed each page of the contract and signed the contract as Ian Freeman, Minister, Shire Free Church, dated December 23, 2015.[11]

32. GeneralBytes provided invoices showing two CVC Kiosks shipped to Ian Freeman and one shipped to "Shire Free Church." GeneralBytes also identified additional parties associated with Freeman that sought assistance with the software on devices associated with Freeman's account and other devices included in the chart in paragraph 30 operated by "Shire" entities.

33. For example, Derrick J. Freeman contacted GeneralBytes via the GeneralBytes cloud server and its online chat platform regarding technical issues with devices purchased by Freeman and other bitcoin devices. In one such message on August 2, 2018, Derrick Freeman said that he had received "a couple notifications about unpaid invoices" but that his "partner says he paid those invoices" and that his "partner, Steven Zeiler, is the one listed on the account." In its subpoena response, GeneralBytes indicated that four of the bitcoin machines that Derrick Freeman inquired about were probably owned previously by Steven Zeiler. GeneralBytes

[11] As a result, I am seeking to search email accounts dating back to November 2015.

provided the following email addresses for Zeiler: me@stevenzeiler.com and zeiler.steven@gmail.com.

34. Derrick Freeman's cell phone number was also listed on advertisements on a CVC kiosk at the Free State Bitcoin Shoppe in Portsmouth. This phone number was the point of contact for making appointments to access the CVC kiosk and for any questions regarding virtual currency.

35. The "Shire" web-page, https://shiresociety.com/crypto/, describes Freeman's network of "Shire Crypto Vending" machines (CVM) in the State of New Hampshire to sell "Bitcoin and other cryptocurrencies." The website describes the "CVMs" as follows:

> It's important to note that the church's Crypto Vending Machines are not ATMs, though many confuse the two terms. The machines sell a digital product, cryptocurrency, for cash, like any other vending machine. The CVMs are one-way. They just vend, they don't buy crypto or dispense cash. The machines are stocked with crypto and sell from that stock. The CVM is not making purchases for the customer on an exchange. Machines that do that have ridiculous identification requirements. Your crypto is your business and as a customer of the church, your privacy is respected. (While our machine does not require identification, there is security monitoring the premises.)

36. In May 2019, I spoke with an Enforcement Specialist at FinCEN who informed me that the "Shire Crypto Vending" machines are CVC kiosks that must be licensed with FinCEN because Freeman's CVC kiosks are electronic terminals which accept currency, in this case U.S. cash, and transmit the equivalent value in bitcoin.

37. Freeman's CVC kiosks, however, are not licensed with FinCEN. In August 2019, at my request, FinCEN searched certified Bank Secrecy Act records. The search showed that that between January 1, 2001, and August 19, 2019, none of the six CVC kiosks listed above and owned by Freeman and the Shire Free Church were licensed as money service transmitters.

Undercover Purchases of Bitcoin from the CVC Kiosks

38. As detailed below, FBI Agents used U.S. currency to make purchases of Bitcoin at all of the CVC kiosks listed in paragraph 29. The details of these transactions are as follows.

39. On July 21, 2018, UC1 completed a bitcoin transaction at the CVC kiosk located at the Seacoast Rep Theater, 125 Bow Street, Portsmouth, New Hampshire, 03801. UC1 paid $200 in United States Currency and received bitcoin in a Bitcoin wallet controlled by the FBI (the "FBI Wallet").

40. On August 3, 2018, UC1 completed a bitcoin transaction at the CVC kiosk located at Area 23, 254 North State Street, Concord, New Hampshire, 03301. A sign was posted next to the CVC kiosk stating the device was independently owned and managed by Shire Cryptocoin. The sign describes the device as a cryptocurrency vending machine and not an ATM and provides step by step directions on how to use the device. The email address provided on the sign was **shirecryptocoin@gmail.com**. UC1 paid $500 in United States Currency and, in exchange, received bitcoin in the FBI Wallet.

41. On August 9, 2018, UC1 completed a bitcoin transaction at the CVC kiosk located at Murphy's Taproom, 494 Elm Street, Manchester, New Hampshire, 03101. UC1 paid $500 in United States Currency and received bitcoin in the FBI Wallet.

42. On August 14, 2018, UC1 completed a bitcoin transaction at the CVC kiosk located at Thirsty Owl, 141 Winchester Street, Keene, New Hampshire, 03431. A sign posted next to the kiosk indicated that it was updated as of August 2018, and listed contact information as **KeeneCrypto@gmail.com**. UC1 paid $220 in United States Currency and, in exchange, received bitcoin in the FBI Wallet.

43. On August 16, 2018, UC1 completed a bitcoin transaction at the CVC kiosk located at Port City Coin and Jewelry, 599 US 1 Portsmouth, New Hampshire, 03801. UC1 paid $220 in United States Currency and, in exchange, received bitcoin in the FBI Wallet.

44. On August 20, 2018, UC1 completed a bitcoin transaction at the CVC kiosk located at Uncommon Goods Route 101, 661 Marlboro Street, Keene, New Hampshire, 03431. A sign next to the machine listed contact information as **KeeneCrypto@gmail.com**. UC1 paid $200 in United States Currency and, in exchange, received bitcoin in the FBI Wallet.

45. Information within the FBI Bitcoin wallet allows the person with access to the wallet to conduct a blockchain analysis of the transactions made by the FBI at the identified CVC kiosks. Investigators then review this data to identify other Bitcoin wallet identifiers and sources of the bitcoin transferred to the FBI wallet. According to a blockchain analysis by the FBI, five of the CVC kiosks received a portion of their bitcoin supply from the same Bitcoin Wallet (the "Freeman Wallet""). These five kiosks were located at the following locations: Murphy's Taproom, Port City, Route 101 Goods, Seacoast Rep., and Thirsty Owl.

Funding of the ATM Bitcoin Holding Wallet (Freeman Wallet)

46. The investigation has revealed that the Freeman Wallet is funded by several bank accounts associated with Ian Freeman. Coinbase records show that the Freeman Wallet received bitcoin from an account at Coinbase, Inc. Coinbase is a virtual currency exchange. The Coinbase account that funded the Freeman Wallet was in the name of Shire Free Church and created by Ian Bernard. The New Hampshire driver's license on file for the Coinbase account was for Ian B Freeman. The email addresses associated with this Coinbase account are **ian@freetalklive.com**

and **Shirebtc@gmail.com**.[12] Records from Coinbase indicate that Freeman's account was closed by Coinbase because of suspected unlawful activity. I believe that there may be communications between Freeman and Coinbase about the account closure on the email addresses Freeman provided to Coinbase for his account. Such communications are likely to show that Freeman had knowledge about the illegal nature of his business.

47. Coinbase records show that the Coinbase account was funded by bank accounts at Cheshire County Federal Credit Union and Bank of America. Records from Cheshire County FCU show that the account that funded the Coinbase account is in the name of Ian B Freeman d/b/a Free Talk Live and list email accounts lnedgington@yahoo.com and **shirebtc@gmail.com**. Bank of America records list that account in the name of Shire Free Church Monadnock.

48. ItBit, Inc. records show that the Freeman Wallet received bitcoin from three accounts at itBit, Inc. itBit, Inc. is a virtual currency exchange. These accounts were in the names of Ian Freeman, Andrew Spinella, and Renee LeBlanc.

49. I know that Spinella and LeBlanc are associates of Freeman. I received information about suspicious activity in bank accounts used by Spinella and spoke with Spinella about the activity. Spinella told me that his girlfriend, Renee LeBlanc, introduced him to Freeman and that Freeman asked Spinella to open bank accounts for Freeman to use for his Bitcoin business because his own accounts had been closed.

[12] According to open source web based domain search sites, the email accounts ending in the "freetalklive.com" registered domain is hosted by NameCheap. The IP associated with this domain appears to be hosted through Google, Inc. Therefore, I believe that records associated with this email address may be held by both NameCheap and Google.

50. The email accounts associated with the itBit account were **chaosdragoon77@yahoo.com, ian@freetalklive.com, shirebtc-itbit@gmail.com**, and **bitcoinbombshell727@gmail.com**. The itBit accounts were funded by State Farm Bank, Allied Bank, JP Morgan Chase and Bank of America. Bank records show that the State Farm Bank account was in the name of Ian Freeman. Allied Bank was in the name of Ian B. Freeman and associated with the e-mail address of **ian@freetalklive.com**. JP Morgan Chase and Bank of America accounts were in the name of Shire Free Church Monadnock. Records from itBit indicate that Freeman's account was closed by itBit because of suspected unlawful activity. I believe that there may be communications between Freeman and itBit about the reasons for the account closure on the email addresses Freeman provided to itBit for his account. Such communications are likely to show that Freeman had knowledge about the illegal nature of his business.

51. Subpoenaed records from Gemini Trust show that the Freeman Wallet received bitcoin from two accounts at Gemini Trust Company LLC. Gemini Trust is a virtual currency exchange. These accounts were in the names of Freeman and LeBlanc. The email accounts associated with these accounts were **ian+gemini@freetalklive.com** and **bitcoinbombshell727@gmail.com**. The Gemini accounts were funded by accounts at Axos Bank, Compass Bank and Digital Federal Credit Union. Bank records show that the Axos Bank account was in the name of Ian B. Freeman and associated with the e-mail address of **ian@freetalklive.com**. The Compass Bank account was in the name of Ian Freeman. The Digital Federal Credit Union account was in the name of Ian Freeman and associated with the e-mail address of **ian@freetalklive.com**. Records from Gemini indicate that Freeman's account was closed by Gemini because of suspected unlawful activity. I believe that there may be

communications between Freeman and Gemini about the account closure on the email addresses Freeman provided to Gemini for his account. Such communications are likely to show that Freeman had knowledge about the illegal nature of his business.

52. Localbitcoins.com is a peer to peer Bitcoin exchange. It is an online marketplace where individuals can buy, sell and trade Bitcoin with each other. The site allows users to post advertisements where they state exchange rates and payment methods for buying or selling bitcoins. The advertisements allow clients to reply to these advertisements and agree to meet in person to buy bitcoins with cash, or trade directly with online banking. Bitcoins are placed in Localbitcoins.com web wallet and transferred through the site to purchasers. Records from LocalBitcoins.com show that the Freeman Wallet sent bitcoin to LocalBitcoins.com. The LocalBitcoins.com accounts belonged to usernames "FTL_Ian" and "ShireBTC." The email accounts associated with these users were **ian@freetalklive.com** and **shirebtc+lbc@gmail.com**. I know that localbitcoins.com sends copies of conversations on the website to the email address or addresses associated with the account. Therefore, I believe that communications Freeman had with Bitcoin customers on localbitcoins.com will also be stored on these email accounts.

Fraud Victims and Freeman's Bank Accounts

53. FBI Agents and other law enforcement officers around the United States interviewed individuals who deposited money into bank accounts associated with Freeman, his associates, and the Shire Free Church. Many of these individuals were victims of online schemes of various types. Others deposited money into Freeman's bank account in order to purchase bitcoin. None of the individuals interviewed to date knew Freeman or were donating money to the Shire Free Church.

54. On May 16, 2019, an FBI agent interviewed S.D. at S.D.'s residence in Ohio. S.D. is a widow who, at some point after the death of her husband in July 2017, started an online relationship with a David Brusch who told her that he was going to purchase diamonds in South Africa. Brusch convinced S.D. to "get cash and forward it to people to buy Bitcoin." When shown a copy of a $25,000 transfer she made to "Ian Freeman," S.D. said this transfer of money was done at Brusch's direction. S.D. does not know Freeman or the Shire Free Church.

55. On May 5, 2019, an FBI agent interviewed J.C. at J.C.'s residence in North Carolina. J.C. said that she met Adam Karlsson on match.com in June 2018. At Karlsson's direction, she subsequently sent money to "Ian Freeman" to "help" Karlsson and in return for his promise to come to North Carolina and have a relationship with her. J.C. deposited a total of $36,000 in Freeman's bank account. J.C. stated that Karlsson "swindled" her out of her money. J.C. does not know Freeman or the Shire Free Church.

56. On July 15, 2019, an FBI agent interviewed D.B. at D.B.'s residence in Ohio. He recalled that in 2017, he was scammed out of money on multiple occasions and as part of the scam he specifically remembered sending money to the Shire Free Church. This scheme involved fraudulent "investments" and D.B. was instructed by the scammers online to send money to the Shire Free Church to "cover attorney fees." All of the money that D.B. lost in this scheme was money he "borrowed" from other people. D.B. does not know Freeman or the Shire Free Church.

57. On July 15, 2019, an FBI agent interviewed K.C.at K.C.'s residence in Tennessee. Earlier in 2019, K.C. was involved in a lottery scheme where she was instructed by scammers to open a bank account at SunTrust Bank. K.C. received checks from the scammers who instructed her to send the funds from these checks to "Ian Freeman." K.C. then sent money to Freeman at Axos Bank. K.C. does not know Freeman or the Shire Free Church.

58. On May 10, 2019, an FBI agent interviewed C.J. at C.J.'s place of employment in Pennsylvania. In approximately January 2019, C.J. began an online relationship with a Jude Goible. Goible convinced C.J. to send $175,000 of her money to help him out so they could be together. Goible instructed C.J. to deposit her money into various bank accounts. When shown a copy of her deposit slip into an account in the name of "Ian Freeman" C.J. explained that she deposited money at the direction of Goible, the scammer. C.J. does not know Freeman or the Shire Free Church.

59. On September 5, 2018, an FBI agent interviewed S.E. at S.E.'s residence in New Hampshire. S.E. met Michael Burnam through Facebook and started an online romantic relationship with him that, at the time of the interview, had lasted about five years. Michael asked S.E. to accept wire transfers from him and then move this money to other accounts. For example, Michael asked S.E. to accept cash that he mailed to her, approximately $25,000, and then instructed her on how to use the CVC kiosks to convert this cash to bitcoin. He specifically directly S.E. to use the CVC kiosk located at Uncommon Goods in Keene, NH owned by Ian Freeman and the Shire Free Church (the same CVC kiosk at 661 Marlboro Road in Keene, NH 03431 listed in paragraph 29). S.E. does not know Freeman or the Shire Free Church.

60. On April 14, 2018, an FBI agent interviewed M.F. at a business near her residence in Michigan. In approximately March 2018, M.F. was contacted by a David Brusch, whom she met through an online dating website. Eventually M.F.'s relationship with Brusch became romantic, although she never met him in person. Brusch asked M.F. to transfer him money so it could "clear customs." On one occasion, Brusch instructed M.F. to transfer some of this money to an account bearing the name, "Shire Free Church." M.F. did research and knows now that

Brusch scammed her into making these transfers and sending him her money. M.F. does not know Freeman or the Shire Free Church.

61. According to police reports, in late 2018 a medical doctor who lives in Alabama, D.T., fell victim to a scheme where he was told he "needed to send money to a friend whom was arrested." D.T. was instructed by the scammer and later sent $4,020.13 to a GFA Credit Union account in the name of "Colleen Fordham." D.T. filed a police report with his local department, which in turn called the Gardner Massachusetts Police Department because the bank account for Colleen Fordham was based in that area. The Gardner Police officer who received this report from Alabama started making inquiries about Fordham. The Gardner Police officer spoke with GFA about this fraud and GFA Credit Union decided to freeze the $4,012.13 in Fordham's account until this matter could be resolved.

62. On January 9, 2019, the aforementioned Gardner Police Officer received a call from a male who identified himself as "Ian Freeman from the Shire Free Church in Keene, New Hampshire." Freeman claimed to be representing Colleen Fordham and inquired as to why the officer was asking about Fordham. The officer's report states in part,

> From speaking with Freeman, he seemed to have direct knowledge of the situation, specifically the reported fraud associated with the account. Freeman said that Fordham initially believed the check was sent legitimately in exchange for Bitcoin.

Freeman said he would set up a time for the officer to talk to Fordham. After several attempts by the officer to talk to Fordham, she never met with him.

63. GFA Credit Union ended up returning the $4,012.13 to D.T. after Colleen Fordham, through her attorney, gave a notarized statement to GFA Credit Union acknowledging the fraudulent activity on her account.

64. I believe that Freeman is operating illegal money transmitting businesses, through his unregistered ATMs and perhaps through his sales of Bitcoin over Localbitcoins.com or otherwise. I also believe that Freeman has received the proceeds of fraudulent schemes in his bank accounts and that he has provided bitcoin in exchange for those funds. I believe that the email accounts listed herein will provide evidence of those offenses. I seek to search email accounts affiliated with Freeman's CVC kiosks (keencrypto@gmail.com, shirecryptocoin@gmail.com, ian@freetalklive.com and steven@anypayinc.com), which may contain communications with bitcoin purchasers about issues with the kiosks, sources of the cash used to make bitcoin purchases, and/or manufacturers of the kiosks. I also seek to search email accounts associated with virtual currency exchange accounts (bitcoinbombshell727@gmail.com, shiretc@gmail.com, shirebtc-itbit@gmail.com, ian+gemini@freetalklive.com, chaosdragon77@yahoo.com) which I believe are likely to contain communications between Freeman and the exchanges about the reason the accounts were closed, how Freeman funded the Bitcoin ATMs, other Bitcoin purchases he made for customers, and Freeman's knowledge of the illegal nature of his business. I also seek to search emails from the account associated with Freeman's local bitcoins account, (shirebtc+lbc@gmail.com and ian@freetalklive.com), which may contain communications between Freeman and bitcoin purchasers about the source of the funds, and Freeman's knowledge about legal requirements for selling bitcoin.

65. On November 27, 2019, United State Magistrate Judge Andrea K. Johnstone issued warrants to search all of the accounts discussed herein. Due to an oversight, the search warrants were never served on the providers. I am requesting renewed authorization to search these accounts as the previous warrants have since expired.

Background Concerning Email

66. In general, an email that is sent to an email subscriber is stored in the subscriber's "mail box" on the email provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the email provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the email provider's servers for a certain period of time.

67. In my training and experience, I have learned that Google, Yahoo, Amazon, and NameCheap (the "Email Providers") provide a variety of on-line services, including electronic mail ("email") access, to the public. The Email Providers allow subscribers to obtain email accounts at their domain name (e.g., yahoo.com, gmail.com) or host accounts under another domain name (e.g., freetalklive.com, anypayinc.com), like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the Email Provider. During the registration process, the Email Providers ask subscribers to provide basic personal information. Therefore, the computers of the Email Providers are likely to contain stored electronic communications (including retrieved and unretrieved email for the Email Providers' subscribers) and information concerning subscribers and their use of the Email Providers' services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

68. An email subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Email Provider. In my training and experience, evidence of who was using an email account may be found in address

books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

69. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

70. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

71. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

72. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either

inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Conclusion

73. Based on the forgoing, I request that the Court issue the proposed search warrants.

74. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of these warrants. The government will execute these warrants by serving them on Google, Yahoo, Amazon, and NameCheap. Because the warrant will be served on Google, Yahoo, Amazon, and NameCheap, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,

/s/ Kathryn Thibault
Kathryn Thibault
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on December 23, 2019

Honorable Andrea K. Johnstone
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1

Property to Be Searched

This warrant applies to information associated with the following email addresses that are stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California:

Ian+gemini@freetalklive.com
Ian@freetalklive.com
Keenecrypto@gmail.com
Bitcoinbombshell727@gmail.com
Shirebtc+lbc@gmail.com
Shirecryptocoin@gmail.com
Shirebtc@gmail.com
Shirebtc-itbit@gmail.com

ATTACHMENT A2

Property to Be Searched

This warrant applies to information associated with the following email addresses that are stored at premises owned, maintained, controlled, or operated by Yahoo!, Inc., a company headquartered at 701 First Avenue, Sunnyvale, California:

Chaosdragoon77@yahoo.com

ATTACHMENT A3

Property to Be Searched

This warrant applies to information associated with Steven@anypayinc.com that is stored at premises owned, maintained, controlled, or operated by Amazon, a company headquartered at 300 Deschutes Way SW, Ste. 304, Tumwater WA 98501.

ATTACHMENT A4

Property to Be Searched

This warrant applies to information associated with the following email addresses that are stored at premises owned, maintained, controlled, or operated by NameCheap, a company headquartered at 11400 W. Olympic Boulevard, Suite 200, Los Angeles, CA 90064:

Steven@anypayinc.com
Ian+gemini@freetalklive.com
Ian@freetalklive.com

ATTACHMENT B1

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account **from November 1, 2015, to November 27, 2019**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money transmitting business, and of 18 U.S.C. §§ 1956 and 1957, which prohibit money laundering, those violations involving **Ian Freeman aka Ian Bernard, Derrick Freeman aka Derick Horton, Steven Zeiler, Andrew Spinella, Renee LeBlanc, and Colleen Fordham** and occurring after **November 1, 2015**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies in exchange for U.S. or other currencies over the Internet, through the postal service, in person, over wire/bank transfer, or via other methods.

(b) The operation and scope of an unlicensed money service business involving Bitcoin and/or other digital currencies.

(c) The maintenance and operation of digital currency (including Bitcoin) "wallets" and/or any other means of digital currency storage.

(d) The use of the CVC kiosks or Freeman's bank accounts to launder proceeds of criminal conduct.

(e) Any financial institution account (including accounts at banks, credit unions, and digital currency exchanges) that is owned by, controlled by, or otherwise accessible to Freeman, whether as an individual or acting on behalf of a business entity, including:

i. JP Morgan Chase

ii. Bank of America

iii. Allied Bank

iv. Digital Federal Credit Union

v. Axos Bank

vi. Cheshire County Federal Credit Union

(f) The purchase of personal assets, including estate, vehicles, boats, jewelry, and precious metals as proceeds of the unlawful activity discussed herein.

(g) The existence, identity, and travel of other parties involved with Freeman in the purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies.

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

(i) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation, including knowledge of the source of funds transferred to Freeman's accounts or used to purchase digital currency from Freeman's CVC kiosks.

(j) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Google**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Google**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Google**, and they were made by **Google** as a regular practice; and

b. such records were generated by **Google's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Google** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Google**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature

ATTACHMENT B2

Particular Things to be Seized

I. Information to be disclosed by Yahoo! Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account **from November 1, 2015, to November 27, 2019**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money transmitting business, and of 18 U.S.C. §§ 1956 and 1957, which prohibit engaging in monetary transactions in property derived from specified unlawful activity, those violations involving **Ian Freeman aka Ian Bernard, Derrick Freeman aka Derick Horton, Steven Zeiler, Andrew Spinella, Renee LeBlanc, and Colleen Fordham** and occurring after **November 1, 2015**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies in exchange for U.S. or other currencies over the Internet, through the postal service, in person, over wire/bank transfer, or via other methods.

(b) The operation and scope of an unlicensed money service business involving Bitcoin and/or other digital currencies.

(c) The maintenance and operation of digital currency (including Bitcoin) "wallets" and/or any other means of digital currency storage.

(d) The use of the CVC kiosks or Freeman's bank accounts to launder proceeds of criminal conduct.

(e) Any financial institution account (including accounts at banks, credit unions, and digital currency exchanges) that is owned by, controlled by, or otherwise accessible to Freeman, whether as an individual or acting on behalf of a business entity, including:

i. JP Morgan Chase

ii. Bank of America

iii. Allied Bank

iv. Digital Federal Credit Union

v. Axos Bank

vi. Cheshire County Federal Credit Union

(f) The purchase of personal assets, including estate, vehicles, boats, jewelry, and precious metals as proceeds of the unlawful activity discussed herein.

(g) The existence, identity, and travel of other parties involved with Freeman in the purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies.

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

(i) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation, including knowledge of the source of funds transferred to Freeman's accounts or used to purchase digital currency from Freeman's CVC kiosks.

(j) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Yahoo! Inc. ("Yahoo")**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Yahoo**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Yahoo**, and they were made by **Yahoo** as a regular practice; and

b. such records were generated by **Yahoo's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Yahoo** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Yahoo**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature

ATTACHMENT B3

Particular Things to be Seized

I. Information to be disclosed by Amazon (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account **from November 1, 2015, to November 27, 2019**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money transmitting business, and of 18 U.S.C. §§ 1956 and 1957, which prohibit engaging in monetary transactions in property derived from specified unlawful activity, those violations involving **Ian Freeman aka Ian Bernard, Derrick Freeman aka Derick Horton, Steven Zeiler, Andrew Spinella, Renee LeBlanc, and Colleen Fordham** and occurring after **November 1, 2015**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies in exchange for U.S. or other currencies over the Internet, through the postal service, in person, over wire/bank transfer, or via other methods.

(b) The operation and scope of an unlicensed money service business involving Bitcoin and/or other digital currencies.

(c) The maintenance and operation of digital currency (including Bitcoin) "wallets" and/or any other means of digital currency storage.

(d) The use of the CVC kiosks or Freeman's bank accounts to launder proceeds of criminal conduct.

(e) Any financial institution account (including accounts at banks, credit unions, and digital currency exchanges) that is owned by, controlled by, or otherwise accessible to Freeman, whether as an individual or acting on behalf of a business entity, including:

i. JP Morgan Chase

ii. Bank of America

iii. Allied Bank

iv. Digital Federal Credit Union

v. Axos Bank

vi. Cheshire County Federal Credit Union

(f) The purchase of personal assets, including estate, vehicles, boats, jewelry, and precious metals that represent the proceeds of unlawful activity discussed herein.

(g) The existence, identity, and travel of other parties involved with Freeman in the purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies.

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

(i) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation, including knowledge of the source of funds transferred to Freeman's accounts or used to purchase digital currency from Freeman's CVC kiosks.

(j) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Amazon**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Amazon**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Amazon**, and they were made by **Amazon** as a regular practice; and

b. such records were generated by **Amazon's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Amazon** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Amazon**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature

ATTACHMENT B4

Particular Things to be Seized

I. Information to be disclosed by NameCheap (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account **from November 1, 2015, to November 27, 2019**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money transmitting business, and of 18 U.S.C. §§ 1956 and 1957, which prohibit engaging in monetary transactions in property derived from specified unlawful activity, those violations involving **Ian Freeman aka Ian Bernard, Derrick Freeman aka Derick Horton, Steven Zeiler, Andrew Spinella, Renee LeBlanc, and Colleen Fordham** and occurring after **November 1, 2015**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies in exchange for U.S. or other currencies over the Internet, through the postal service, in person, over wire/bank transfer, or via other methods.

(b) The operation and scope of an unlicensed money service business involving Bitcoin and/or other digital currencies.

(c) The maintenance and operation of digital currency (including Bitcoin) "wallets" and/or any other means of digital currency storage.

(d) The use of the CVC kiosks or Freeman's bank accounts to launder proceeds of criminal conduct.

(e) Any financial institution account (including accounts at banks, credit unions, and digital currency exchanges) that is owned by, controlled by, or otherwise accessible to Freeman, whether as an individual or acting on behalf of a business entity, including:

i. JP Morgan Chase

ii. Bank of America

iii. Allied Bank

iv. Digital Federal Credit Union

v. Axos Bank

vi. Cheshire County Federal Credit Union

(f) The purchase of personal assets, including estate, vehicles, boats, jewelry, and precious metals that represent the proceeds of the illegal activity discussed herein.

(g) The existence, identity, and travel of other parties involved with Freeman in the purchase, transfer, sale, or advertisement of Bitcoin or other digital currencies.

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

(i) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation, including knowledge of the source of funds transferred to Freeman's accounts or used to purchase digital currency from Freeman's CVC kiosks.

(j) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **NameCheap**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **NameCheap**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **NameCheap**, and they were made by **NameCheap** as a regular practice; and

b. such records were generated by **NameCheap's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **NameCheap** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **NameCheap**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature